UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

subject premises located at 1627 Erie Street, Racine, WI 53402

Case No. 25 MJ 71

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2251(a)	Production of Child Pornography
18 USC 2252	Possessing and Distributing Child Pornography

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KEVIN C WRONA
Digitally signed by KEVIN C WRONA
Date: 2025.06.04 13:43:19 -05'00'

Applicant's signature

Kevin Wrona, Special Agent HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/04/2025

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kevin C. Wrona, having been duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since 2010, and am currently assigned to HSI Office of the Resident Agent in Charge, Milwaukee, Wisconsin. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, as well as through information provided to me by other law enforcement officers whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and search warrants. I believe this information is reliable because it was provided by independent companies in response to court or agency requests.

3. Based upon the information described below, I submit probable cause exists to believe that an individual used the internet at 1627 Erie Street, Racine,

Wisconsin 53402 (subject premises), more particularly described in Attachment A, and has committed the crimes of possessing and distributing child pornography, in violation of 18 U.S.C. § 2252, and production of child pornography, in violation of 18 U.S.C. § 2251, and evidence relating to these crimes, more particularly described in Attachment B, can be found at the subject premises.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a) "Camera" means a device used for recording visual images in the form of photographs, film, or video signals. Digital cameras record and store images in a digital format, which can include Digital8, MiniDV, DVD, a hard drive, or solid-state flash memory.

b) "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text

messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

c) "Child erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d) "Child pornography" is defined in 18 U.S.C. § 2256(8), as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e) "Cloud" or "cloud storage" is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instated of the (user's) computer's hard drive. The internet provides the connection between the user's computer and the database for saving and retrieving files.

f) "Computer" is defined pursuant to 18 U.S.C. § 1030€(1) as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices.

g) "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h) "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys,

which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i) Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j) "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k) "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB thumb drives). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

l) "File Transfer Protocol" (FTP) is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

m) A "hash value" is a unique alphanumeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A

hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

n) "Internet Protocol address" or "IP address" refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

o) "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

p) "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment

connecting a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter. This MAC address is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

q) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r) "Records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

t) A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u) "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols

in a standard form. People use URLs on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v) A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

w) Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

x) Exchangeable Image File Format "EXIF" is a standard that specifies formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. The metadata tags defined in the Exif standard cover a broad spectrum to include, camera settings: This includes static information such as the camera model and make, and information that varies with each image such as orientation (rotation), aperture, shutter speed, focal length, metering mode, and ISO speed information; image metrics: Pixel dimensions, resolution, colorspace, and filesize; date and time information, digital cameras will record the current (local) date and time

set on the device; location information; a thumbnail image for previewing the picture on the camera's LCD screen, in file managers, or in photo manipulation software; Descriptions; and copyright information.

USE OF COMPUTERS AND CELL PHONES FOR CHILD PORNOGRAPHY

6. I have personally been involved with several child exploitation investigations, and have personally interviewed offenders, executed search warrants, and reviewed the fruits of those searches and seizures to observe numerous examples of child pornography, as defined at 18 U.S.C. § 2256. I have also consulted with other law enforcement officers who investigate the sexual exploitation of children. Based on my training and experience, I have learned individuals who receive and collect child pornography may receive sexual gratification, stimulation, and satisfaction viewing children engaged in sexual activity, in sexually suggestive poses such as in person, in photographs, other visual media, or from literature describing such activity. Individuals who receive and collect child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a computer in a private residence, allows the collectors the opportunity to safely maintain their collections for many years and enable the collector to frequently view the collection, which is highly valued.

7. Computers and other devices that can connect to the Internet are capable of sending and receiving images, videos, and other files to users around the world, including digital images of child pornography. In particular, the large storage capacities of computers and other digital media storage devices make them ideal repositories for images and videos of child pornography. Devices capable of storing such files include external hard drives, video game consoles, smartphones, and digital media players, which all have the ability to store digital data, access the Internet, and send or receive digital data electronically. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and more recently in mobile smartphones has grown tremendously within the last several years. These drives can store thousands of images at very high resolutions. As a result, computers and other digital devices that are used to send, receive, or store child pornography often contain evidence of that activity.

8. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or smart phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's devices. Even in cases where

online storage is used, evidence of child pornography can be found on the user's computer devices in most cases.

9. As with most digital technology, communications made from a computer or smart phone are often saved or stored on that device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file

or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's type of device, operating system, storage capacity, and computer habits.

CHAT APPLICATION A[1]

10. Chat Application A is an encrypted chat application available for both mobile and desktop devices, and it can run on iOS, Android, and Windows operating systems. Users do not need to provide a phone number or email address to create an account on Chat Application A. Its website boasts that Chat Application A protects data through end-to-end encryption, does not retain any metadata or IP addresses, and only stores messages until their delivery. Because of this encryption, certain information often obtainable from other companies that provide online communication services –

[1] The name of Chat Application A is known but not being disclosed herein to protect operational security and decrease the likelihood investigations involving Chat Application A become prematurely known by its users. These and other sensitive operational details have been omitted from this affidavit.

such as email addresses, phone numbers, and logs of IP addresses – is not obtainable from the company behind Chat Application A.

11. The above-described encryption means users of applications like Chat Application A are difficult to identify. The privacy and protection provided by encrypted chat applications makes them popular among those engaged in producing, distributing, receiving, and possessing sexually explicit content depicting children. Users of these applications often know they can operate with a higher level of anonymity than they can on unencrypted messaging applications.

12. Chat Application A does, however, use "push tokens." A push token is a unique identifier generated by Apple (iOS) and Google (Android) smart phones. These push tokens allow applications to "push" notifications – such as new incoming messages – to users' smart phones. From my training and experience, I know a push token can be used to identify the device(s) on which an individual has installed Chat Application A and receives push notifications from the application.

13. Chat Application A assigns users unique identification numbers, and users can choose usernames and communicate with each other in groups or one on one. When invited to a group on Chat Application A, a user must accept the invitation before becoming a member of the group. Users of Chat Application A do not have to actively participate in groups of which they are a member to receive messages and media shared by other users.

PROBABLE CAUSE

14. On June 4, 2025, Homeland Security Investigations (HSI) Milwaukee, WI received information from HSI Attache The Hague related to online undercover activity being conducted by Dutch authorities with an individual on the Chat Application A application with the username "Fantastic" and Chat Application A ID "V45MQX2FG".

15. On June 3, 2025, during an online undercover investigation on the Chat Application A, Dutch authorities observed user "Fantastic" asking, "Any pedo dads wanna share stories and content that we do with our daughters'. This message was posted in a Chat Application A group named "No Limit, Everything Allowed." After seeing this post, the undercover Dutch officer messaged "Fantastic". During the conversation, "Fantastic" stated he was based in the United States, and he has a "4 year old daughter ive started training her into becoming my lil cum dump." After stating this, "Fantastic" sent the undercover Dutch officer a 12 second video that depicted a prepubescent female child, who appeared to be approximately four (4) years old, touching and licking the erect penis of an adult male. When the undercover Dutch officer asked about the child, "Fantastic" confirmed that the girl in the video was "the little princess."

16. HSI The Hague provided the video shared by "Fantastic" to HSI Milwaukee, and I reviewed the video and confirmed that the description of the video does match the content of the video.

17. Using law enforcement tools, Dutch authorities were able to obtain several internet protocol (IP) addresses for user "Fantastic", including 99.149.138.158, and 12.75.40.91. According to internet research done by Dutch authorities, IP address 99.149.138.158 resolved to internet service provider (ISP) AT&T, while IP address 12.75.40.91 resolved to a cellular phone, which could not be resolved. HSI The Hague made an exigent request to AT&T, requesting subscriber information on IP address 99.149.138.158. AT&T telephonically identified the subscriber as, Jocelyn Rosario, with a service address of, 1627 Erie Street, Racine, Wisconsin 53402, with a reported email address of, smith_nelson@yahoo.com.

18. Additional investigative efforts by HSI The Hague into the smith_nelson@yahoo.com email address identified Nelson Smith. Both Rosario and Smith have current Wisconsin driver's licenses with the same address in Silver Lake, WI, however open-source database checks show Rosario with the 1627 Erie Street, Racine, WI as a recent associated address.

19. HSI The Hague further conducted a search on the real estate website Zillow of the 1627 Erie Street address and found several photographs of the property. A review of the photographs found that the general shape, color and condition of the baseboard appeared to be visually identical to those seen in the shared abuse video.

20. HSI The Hague ran the video through a program that can read the Exchangeable Image File Format (EXIF) data contained in the video file and found that the indicated the video was created on April 26, 2025.

21. Open-source checks found Facebook pages for both Jocelyn Rosario and Nelson Smith. A review of the publicly available photographs shared on both Rosario's and Smith's pages found pictures of a minor female who appears to be visibly identical to the minor victim in the shared abuse video.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that forensic examiners can recover computer files or remnants of such files months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how an individual has used a computer, what the person used it for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that an individual viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-

mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which the computer created them, although it is possible for a user to later falsify this information.

b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when someone accessed or used the computer or storage media. For

example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records sought, a review team cannot always readily review computer evidence or data in order to pass it along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a person used a computer, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f) I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because someone used it as a means of committing the criminal offense. The computer is also likely to be a storage

medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain evidence of how the suspect used the computer; sent or received data; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a) Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer

personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched;

b) Searching computer systems requires the use of precise, scientific procedures, which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c) The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d) Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated

and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

25. This is true for several reasons, including the potential volume of evidence. Computer storage devices including cell phones (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

26. There are also technical requirements for supporting this method. Searching computer systems, including cell phones, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the

evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Furthermore, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

27. In light of these concerns, I request authorization to seize the mobile phone, computer hardware, and associated peripherals, more particularly described in Attachment B, that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware, specifically the computer hard drive and mobile phone and any peripherals found, for the evidence described.

USE OF BIOMETRIC FEATURES TO UNLOCK ELECTRONIC DEVICES

28. I also request that this warrant permit law enforcement to compel device owners to unlock a device subject to seizure pursuant to this warrant that is his or her possession or for which law enforcement otherwise has a reasonable basis to believe is used by him or her using the device's biometric features. I seek this authority based on the following:

a) I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b) I believe that one or more of the electronic devices in the subject premises are likely to offer its user the ability to use biometric features to unlock the device(s). For example, I know that some Android devices use fingerprint sensor and/or facial recognition technology to unlock the device.

c) If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's fingerprint sensor, which is typically found as an oval button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to this device.

d) If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. During the registration

process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly.

e) If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

f) In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

g) As discussed in this affidavit, based on my investigation, training, and experience, there is probable cause to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

h) I know from training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with facial recognition if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

29. Due to the foregoing reasons, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and law enforcement otherwise has a reasonable basis to believe has been used to commit the aforementioned offenses, this warrant would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of the owner of the device(s) to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of owner of the device(s) and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of the owner of the device(s) and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

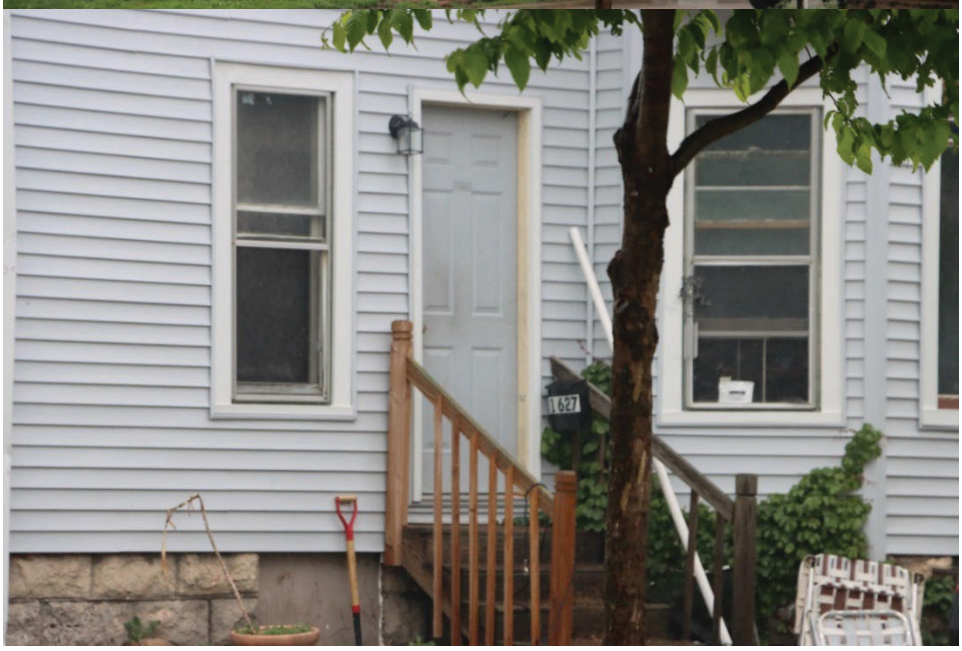
CONCLUSION

30. Based on the facts of the investigation detailed above in this Affidavit, coupled with my training and experience as an HSI Special Agent, I submit there is probable cause to believe that an individual at 1627 Erie Street, Racine, WI 53402 is using an electronic device connected to the internet to produce and distribute CSAM. As such, I submit there is probable cause to believe that in the residence located at 1627 Erie Street, Racine, WI 53402, more particularly described in Attachment A, there exist fruits, instrumentalities and evidence of violations of 18 U.S.C. § 2252 and 2251, as described in Attachment B.

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The **subject premises** is located at **1627 Erie Street, Racine, WI 53402** and is described as a two-story building, with blue/grey siding and grey shingles, with white trim around the windows. The numbers "1627" are affixed to a mailbox on the railing of wooden steps leading to a grey door with white trim.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any computer(s), computer hardware, computer software, removable digital media, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica. Computer as used in this warrant includes mobile phones and smartphones.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, passwords, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C.§ 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C.§ 2256(2).

4. Any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all address books, names, and lists of names and addresses of individuals who may have been in communication by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C.§ 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 225 6(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child

pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online

storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of the owner of the device(s) to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of owner of the device(s) and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of the owner of the device(s) and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
subject premises located at 1627 Erie Street, Racine, WI 53402

Case No. 25 MJ 71

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 06/18/2025 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable William E. Duffin .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 06/04/2025 at 2:45 p.m.

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The **subject premises** is located at **1627 Erie Street, Racine, WI 53402** and is described as a two-story building, with blue/grey siding and grey shingles, with white trim around the windows. The numbers "1627" are affixed to a mailbox on the railing of wooden steps leading to a grey door with white trim.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any computer(s), computer hardware, computer software, removable digital media, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica. Computer as used in this warrant includes mobile phones and smartphones.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, passwords, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C.§ 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C.§ 2256(2).

4. Any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all address books, names, and lists of names and addresses of individuals who may have been in communication by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C.§ 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child

pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online

storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of the owner of the device(s) to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of owner of the device(s) and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of the owner of the device(s) and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.